SNMP Notifications $\longleftrightarrow$ SYSLOG

Jürgen Schönwälder

Jacobs University Bremen

72nd IETF Meeting in Dublin

Introduction

Motivation

- Some operators prefer SNMP notifications, some operators prefer SYSLOG messages
- Some devices generate SNMP notifications, some devices generate SYSLOG messages

Approach

- Provide standards-track mappings between SYSLOG and SNMP using SYSLOG's new structured data elements
- Build on vendor experience with proprietary SYSLOG mappings

Mappings

SNMP → SYSLOG

- Mapping SNMP notifications to SYSLOG messages
  - without loosing machine readable information
  - focusing on the structured data elements
  - leaving the free text message to implementations
- Based on RFC3416 notification format, RFC1157 traps can be dealt with by applying RFC3584

SYSLOG → SNMP

- MIB module for representing SYSLOG messages
  - representation of structured data elements
  - optional SNMP notification to carry SYSLOG content
  - controls to enable notifications or control cache size

Example: SNMP Notification (linkUp)

```
BER Encoding

30:7C
   04:08:80:00:02:B8:04:61:62:63
   04:04:63:74:78:31
   A7:6A
      02:03:6D:08:67
      02:01:00
      02:01:00
      30:5D
         30:0F
            06:08:2B:06:01:02:01:01:03:00
            43:03:01:72:8C
         30:17
            06:0A:2B:06:01:06:03:01:01:04:01:00
            06:09:2B:06:01:06:03:01:01:05:04
         30:0F
            06:0A:2B:06:01:02:01:02:02:01:01:03
            02:01:03
         30:0F
            06:0A:2B:06:01:02:01:02:02:01:07:03
            02:01:01
         30:0F
            06:0A:2B:06:01:02:01:02:02:01:08:03
            02:01:01
```

```
ASN.1 Interpretation

SEQUENCE {
   800002b804616263
   "ctx1"
   SNMPv2-Trap-PDU {
      INTEGER 7145575
      INTEGER 0
      INTEGER 0
      SEQUENCE OF {
         SEQUENCE {
            sysUpTime.0
            94860 }
         SEQUENCE {
            snmpTrapOID.0
            linkUp }
         SEQUENCE {
            ifIndex.3
            3 }
         SEQUENCE {
            ifAdminStatus.3
            up(1) }
         SEQUENCE {
            ifOperStatus.3
            up(1) }
      }
   }
}
```

Example: SYSLOG Message (linkUp)

```
<29>1 2003-10-11T22:14:15.003Z mymachine.example.com
      snmptrapd - ID47
      [snmp ctxEngine="800002b804616263"
            ctxName="ctx1"
            sysUpTime="94860"
            snmpTrapOID="1.3.6.1.6.3.1.1.5.4"
            o="1.3.6.1.2.1.2.2.1.1.3" d="3"
            o="1.3.6.1.2.1.2.2.1.7.3" d="1"
            o="1.3.6.1.2.1.2.2.1.8.3" d="1"]
      linkUp on interface #3
```

- All SNMP data is kept in the `snmp` SD element
- Most varbinds are represented by two SD params; one SD param for the OID and one SD param for the value
- The two special varbinds `sysUpTime.0` and `snmpTrapOID.0` are dealt with using special rules

SYSLOG-MSG-MIB (1/2)

```
+--syslogMsgObjects(1)
   |
   +--syslogMsgControl(1)
   |  |
   |  +-- rwn Unsigned32 syslogMsgTableMaxSize(1)
   |  +-- rwn TruthValue syslogMsgEnableNotifications(2)
   |
   +--syslogMsgTable(2)
   |  |
   |  +--syslogMsgEntry(1) [syslogMsgIndex]
   |     |
   |     +-- --- Unsigned32    syslogMsgIndex(1)
   |     +-- r-n Unsigned32    syslogMsgVersion(4)
   |     +-- r-n DateAndTime   syslogMsgTimeStamp(5)
   |     +-- r-n DisplayString syslogMsgHostName(6)
   |     +-- r-n DisplayString syslogMsgAppName(7)
   |     +-- r-n DisplayString syslogMsgProcID(8)
   |     +-- r-n DisplayString syslogMsgMsgID(9)
   |     +-- r-n OctetString   syslogMsgMsg(10)
   :     +-- r-n Bits          syslogMsgFlags(11)
```

SYSLOG-MSG-MIB (2/2)

```
   :
   +--syslogMsgObjects(1)
   |
   +--syslogMsgSDTable(3)
      |
      +--syslogMsgSDEntry(1) [syslogMsgIndex,syslogMsgSDElementName,\
         :                    syslogMsgSDParamName,syslogMsgSDParamIndex]
         |
         +-- --- DisplayString   syslogMsgSDElementName(1)
         +-- --- DisplayString   syslogMsgSDParamName(2)
         +-- --- Unsigned32      syslogMsgSDParamIndex(3)
         +-- r-n SnmpAdminString syslogMsgSDParamValue(4)


+--syslogMsgNotifications(0)
   |
   +--syslogMsgNotification(1) [syslogMsgFacility,syslogMsgSeverity,\
                                syslogMsgVersion,syslogMsgTimeStamp,\
                                syslogMsgHostName,syslogMsgAppName,\
                                syslogMsgProcID,syslogMsgMsgID,\
                                syslogMsgMsg,syslogMsgFlags]
```

References

V. Marinov and J. Schönwälder.

Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG Messages.
Internet Draft (work in progress) <draft-marinov-syslog-snmp-01.txt>, Jacobs University Bremen, February 2008.

J. Schönwälder, A. Clemm, and A. Karmakar.

Definitions of Managed Objects for Mapping SYSLOG Messages to Simple Network Management Protocol (SNMP) Notifications.
Internet Draft (work in progress) <draft-schoenw-syslog-msg-mib-00.txt>, Jacobs University Bremen, Cisco Systems, April 2008.

R. Presuhn.

Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP).
RFC 3416, BMC Software, December 2002.

J. Case, M. Fedor, M. Schoffstall, and J. Davin.

A Simple Network Management Protocol.
RFC 1157, SNMP Research, PSI, MIT, May 1990.

R. Frye, D. Levi, S. Routhier, and B. Wijnen.

Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework.
RFC 3584, Vibrant Solutions, Nortel Networks, Wind River Systems, Lucent Technologies, August 2003.

R. Gerhards.

The syslog Protocol.
Internet Draft (work in progress) <draft-ietf-syslog-protocol-23.txt>, Adiscon GmbH, September 2007.

SNMP ⟶ SYSLOG Open Issues

- Remove the special case handling of the first two RFC3416 notification varbinds
- Add an optional param carrying the SNMP descriptor for OIDs, for example:

  `o="1.3.6.1.2.1.2.2.1.1.3" l="ifIndex.3" d="3"`
- Need to find the correct SYSLOG way to identify the source of a notification
- Security considerations...

SYSLOG $\longrightarrow$ SNMP Open Issues

- DateAndTime does not provide the resolution of the TIMESTAMP of SYSLOG messages
- Security considerations...

Standardization?

SNMP → SYSLOG

- Is the OPSAWG willing to adopt the SNMP notifications to SYSLOG messages document as WG work item?
- If yes, any SYSLOG/SDE experts willing to get involved to ensure we get the SDEs right?
- Is WG last call after the next IETF a feasible target?

SYSLOG → SNMP

- Is the OPSAWG willing to adopt the SYSLOG-MSG-MIB document as WG work item?
- Is WG last call after the next IETF a feasible target?